Manual de implementación de un mapa de riesgos 2
Introducción 2
Niveles de riesgo: 2
Mapa de riesgos 2
Análisis del contexto 2
- Políticas. 2
- Sociales y culturales. 3
- Económicos. 3
- Seguridad interna y fortalezas. 3
- Incidentes. 3

Atacantes y aliados 3
Análisis de los motivos e intereses de terceros 4
Identificación de riesgos y las vulnerabilidades. 4
Identificación de los niveles de riesgo 5
Metodología 5
Tipos de mapas de riesgos 7
Plan, hábitos, protocolos y uso de herramientas de seguridad 7
Plan de seguridad 7
Elementos del plan: 7
Ejemplo de desarrollo de un plan 7
Protocolos de seguridad 9
Política de seguridad 9
Hábitos de seguridad 9
Herramientas de seguridad 10

Manual de implementación de un mapa de riesgos

Introducción

No todes cumplimos el mismo rol como: líderes comunitarios, defensores ambientales, periodistas o comunicadores, ecologistas, abogados que impulsan casos emblemáticos, etc. No todes enfrentamos el mismo riesgo. No es lo mismo una vulnerabilidad como contraseñas inseguras en una persona de la comunidad; frente a las amenazas del crimen organizado a un líder comunitario.

Niveles de riesgo:

- **Bajo.** Aquellas personas que no manejan información sensible; no son tomadores de decisión o se vinculan a la temática esporádicamente.
- **Medio.** Manejan información privada; sin embargo, la falta de medidas de protección no afecta su vida. Tiene acceso a información de la organización, y las vulnerabilidades pueden afectar la operatividad de la organizción. Sin embargo, no pondrá en riesgo la vida de personas cercanas.
- **Alto.** Aquellos perfiles como: líderes comunitarios, activistas, defensores que toman decisiones sobre la comunidad. Así también periodistas o comunicadores de la región que investigan o reportan sobre delitos ambientales. Otros actores conocidos públicamente con un discurso que denuncia actos de corrupción o que afectan a los derechos humanos. Están expuestos por su propio perfil o rol. Por lo tanto, tienen a mayor posibilidad de ataque o represalias, pues la información que comparten o tienen presenta incomodidad a algún actor como externo.

Mapa de riesgos

Nos permite mapear los riesgos a los que cada persona está expuesto, los posibles peligros o daños.

¿Quién pueden ser un atacante? ¿Cuáles son las debilidades o vulnerabilidades? ¿Las destrezas ante cierta situación? Además, entender las posibles capacidades de los atacantes para poder evaluar mejor el riesgo que representan. Así se puede pensar en las posibles medidas a asumir para eliminar o mitigar el riesgo o exposición, etc.

El mapa de riesgos es una metodología que ayuda a identificar y prevenir posibles daños a la seguridad física, digital y emocional. Se toma en cuenta el contexto de la persona. Se puede realizar un mapa de riesgo de organizaciones. Así conocer riesgos en el entorno digital y físico.

La metodología de mapa de riesgos presenta varios pasos que pueden analizarse de manera paralela:

Análisis del contexto

Este es el primer análisis para realizar. Deben participar las personas que son parte de una organización. Se elije a quienes cumplen un rol más activo y que conocen mejor toda la estructura de contactos, aliados, riesgos, leyes, etc. Se hace un análisis de la coyuntura de la organización y del país:

- Políticas. Normativa vigente del país, leyes, movimientos políticos. ¿Cómo las decisiones políticas pueden afectar el trabajo? ¿Qué personas con las que trabajo pueden verse afectadas por decisiones políticas? ¿La organización puede / quiere recibir financiamiento estatal? ¿Hay legislaciones que afecten el trabajo? ¿Hay censura al trabajo? Prácticas del gobierno frente a los derechos que se pretende defender. ¿Cuáles son los lineamientos gubernamentales sobre la

temática que trabaja la organización? Posibles aliados políticos en el tema, entre otros. Posición de la organización frente a la política estatal.

- Sociales y culturales. ¿Qué percepción tiene la ciudadanía frente a la temática que trabaja la organización? ¿Cuál es el papel de la opinión pública frente a la organización? ¿Quiénes son organizaciones aliadas a nuestro trabajo? ¿Cuáles son personas, instituciones u organizaciones que pueden afectar el trabajo de la organización? ¿Cuál es la capacidad de movilización de la organización? ¿Existen factores históricos o culturales a tomar en cuenta?
- Económicos. ¿Existen disponibilidad de recursos para el desarrollo de la organización? ¿Hay un presupuesto para enfrentar ataques digitales, físicos o emocionales a la organización? ¿Existen donantes a los que la organización pueda acudir en caso de emergencia?
- Seguridad interna y fortalezas. Características del lugar en el que se encuentra la organización. Seguridad de sus oficinas. Seguridad del grupo de personas que integran la organización. Características de la zona y vías de ingreso o evacuación. Presencia de grupos irregulares o que pueden representar un riesgo. Seguridad de los dispositivos que cuentan con información sensible dentro de las oficinas o domicilios; etc. Conocimientos de seguridad física y digital de los miembros de la organización.
- Incidentes. Dentro de la organización han tenido incidentes de seguridad digital o física como: robo de aparatos, virus en las computadoras, robo de información, interceptación de llamadas telefónicas, secuestro, amenazas, incidentes en dispositivos móviles; entre otros.

Otros que por las particularidades del caso puedan constituir puntos para el análisis de riesgo.

Atacantes y aliados

Atacantes. Son quienes constituyen una amenaza a la integridad de la organización. Son actores como: personas, grupos, organizaciones, instituciones, etc. que pueden estar interesados en afectar el trabajo de la organización labor. Pueden ser públicos o privados como: grupos políticos; instituciones de gobierno (nacional o subnacional); servidores públicos; grupos irregulares en la zona; empresas extractivas, entre otros. El objetivo es de tenerlos visibilizados para tener un plan de respuesta en un eventual ataque.

Dentro de los atacantes deberías establecer un perfil de cada uno:

- **Descripción general**. ¿Quién es?
- **Objetivos.** ¿Cuáles son sus metas?
- **Motivación.** ¿Por qué le interesa atacar a la organización?
- **Capacidad técnica**. ¿Qué insumos tiene para hacer daño?
- **Intentos**. ¿Qué intentos previos de ataques registran?
- **Recursos**. ¿Qué recursos financieros y humanos tienen?
- **Limitaciones**. ¿Cuáles son las limitaciones que tienen para ejercer ataques?

Aliados. Mapear aliados con los que ya se cuenta o que ese podría contar. Pues se puede armar un plan de contacto. Entre los aliados están colectivos u organizaciones de sociedad civil o sociales; otros defensores de derechos humanos; organizaciones de la cooperación o internacionales; medios de comunicación; Defensoría del Pueblo, entre otros.

Se puede construir un perfil de un aliado para establecer en qué espacios se puede colaborar o trabajar en colectivo para fortalecer las debilidades:

- Descripción.
- Uso de tecnología.

- Metas.
- Fortalezas.
- Posibles amenazas.
- ¿En qué temáticas confluyen?

Análisis de los motivos e intereses de terceros

Una vez que se tiene claro el perfil de los atacantes y aliados. Ahora es importante entender las motivaciones e intereses. Pensando en la coyuntura y cómo se puede configurar una amenaza.

Las motivaciones e intereses tienen factores: económicos, sociales, políticos, ideológicos, de afectación a los derechos humanos, entre otros.

¿Qué es un ataque focalizado? ¿Qué tipo de motivaciones tiene?

Algunas organizaciones defensoras de derechos humanos han reportado ingreso a sus oficinas; se han llevado equipos de computadora y celulares. Sin embargo, no se llevan impresoras, fax, cámaras u otros objetos de valor. Este es un tipo de ataque focalizado a la organización; la motivación es acceder a información. Seguro afectan a la organización, las personas y/o tema que defienden o a sus miembros. ¿Tienes una estrategia si ocurre esto? ¿Cuál es el plan? ¿Qué perderías? ¿Pones en riesgo a alguien?

Las organizaciones víctimas de este tipo de ataques, les dejan uno o dos dispositivos infectados. O hay software espía en red de Internet de la organización. ¿El atacante ha entrado a la organización, pero no se ha llevado nada? ¿Tuvo acceso al modem de la organización? ¿Ha tenido acceso a un equipo?

Si existe una motivación de extraer información o conocer el trabajo sensible de la organización; se debe analizar posibles escenarios de robo de datos. O implementar protección a los dispositivos.

Identificación de riesgos y las vulnerabilidades.

Deberíamos analizar los riesgos, las vulnerabilidades de la organización ante el contexto, los posibles atacantes, las motivaciones e intereses que tendrían de atacarnos.

Elabora en tu organización una lluvia de ideas con todos los riesgos que puedan pensar:

- Pérdida de celular.
- Robo de datos de la organización.
- Contraseñas inseguras.

Las vulnerabilidades en tres planos: el físico, digital, y emocional. Por ejemplo:

- Falta de conocimiento de la normativa;
- Falta de documentación institucional o que se encuentre vigente;
- Inseguridad física de nuestras instalaciones, las personas, información y equipos;
- No pertenecer a redes de aliados o involucrados en la temática;
- Ausencia de planes de seguridad;
- Falta de planes de acción;
- Falta de recursos.
- Debilidades tecnológicas.
- Falta de capacitación interna y externa sobre seguridad. Entre otros.

Las vulnerabilidades deben estar bien explicadas. Así se puede construir estrategias para mitigar, prevenir, eliminar o reducir ese nivel de riesgo.

Identificación de los niveles de riesgo

Ahora, el siguiente paso es identificar el impacto de determinado riesgo (mayor o menor impacto) y la probabilidad (mayor o menor probabilidad de que ese hecho pueda darse). Es decir, qué tan probable es que roben el celular de la organización; y qué tan grave es que lo roben:

Hecho	Probabilidad	Impacto
Robo de celular	Muy alta	Bajo

- Así será más fácil, saber cuáles hechos son más graves y cuáles no.

Metodología

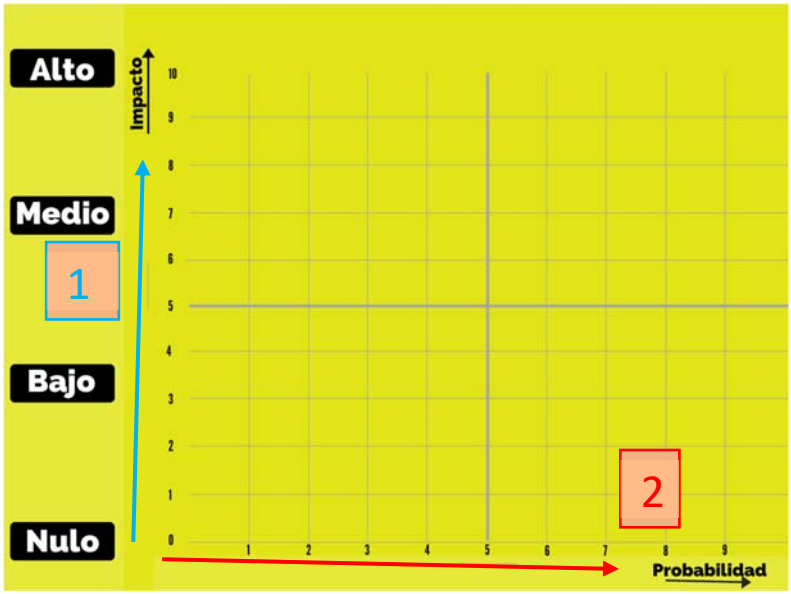
Tras el proceso de identificación contexto, atacantes, vulnerabilidades y niveles de riego. Se va a elaborar una matriz de riesgos para visualizarla y emprender planes de acción.

Materiales:

- Un papelógrafo de 1 metro por 1,50 más a menos. Su tamaño dependerá de las personas que participen. Entre más personas, más ideas, más grande el papelógrafo.
- Marcadores,
- Fichas de papel o cartulina de una cuarta a octava parte de un papel tamaño página A4.

Desarrollo:

Rayarse el papelógrafo como muestra la imagen:



¿Cómo colocar los riesgos en la matriz?

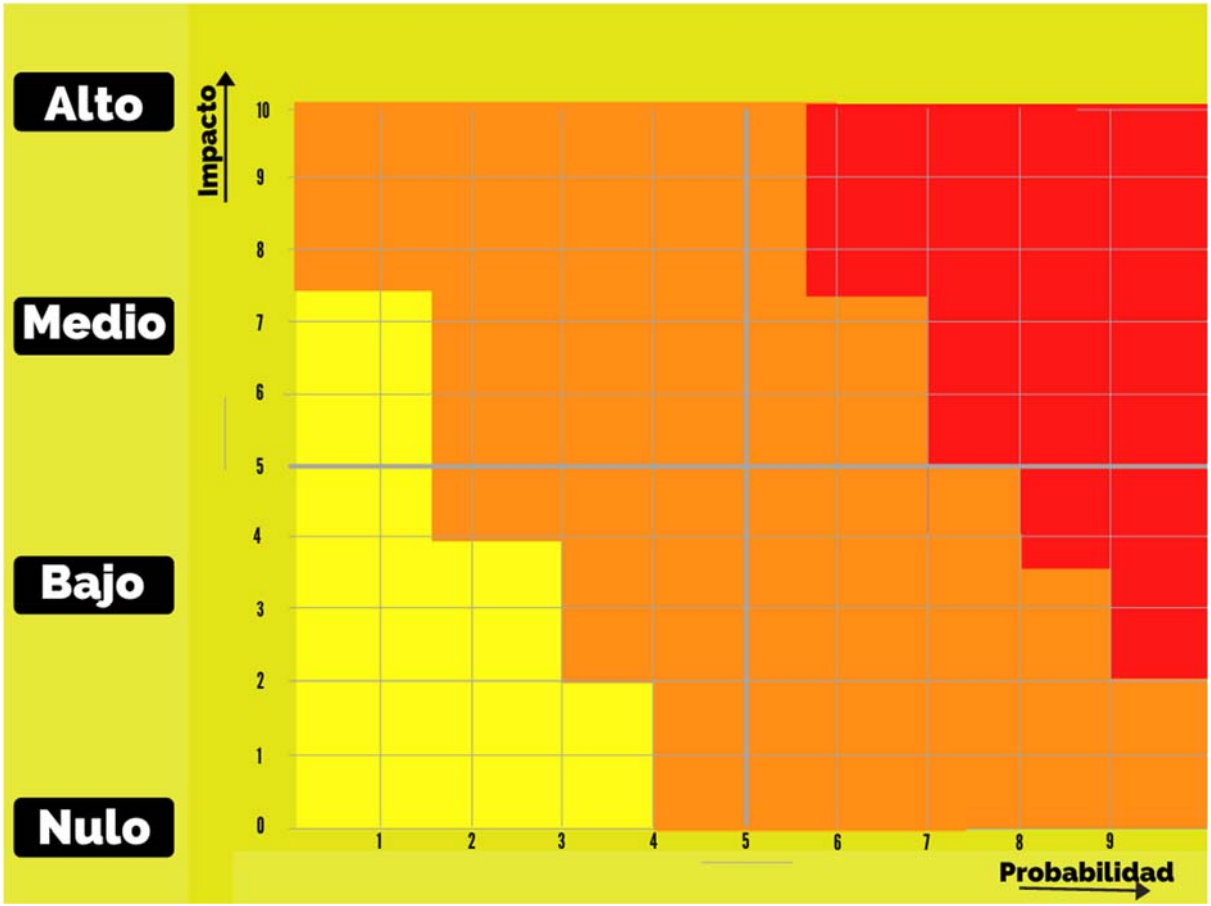
- **El número 1 es vertical y mide el impacto**. Entre más bajo el impacto se le asigna menor valor numérico. Mientras más alto el impacto, mayor el número que se coloca.

- **El número 2 es horizontal y mide la probabilidad.** Ente menos probable que ocurra un hecho es menor el número. Si es más probable que ocurra el hecho es mayor el número.

Una vez que discutimos previamente los riesgos, ahora se va a colocar cada riesgo en un papel, y colocarlo de acuerdo con su nivel de probabilidad e impacto.

Una vez se cuente con ello debe comenzar a llenarse la matriz entendiendo que el 0 involucra menor impacto o probabilidad de realización y 10 el nivel más alto del nivel de impacto (peligro y daño) que puede representar algún hecho de riesgo, circunstancia o vulnerabilidad y una muy alta probabilidad de que esta acción pueda materializarse.

Colores de la matriz

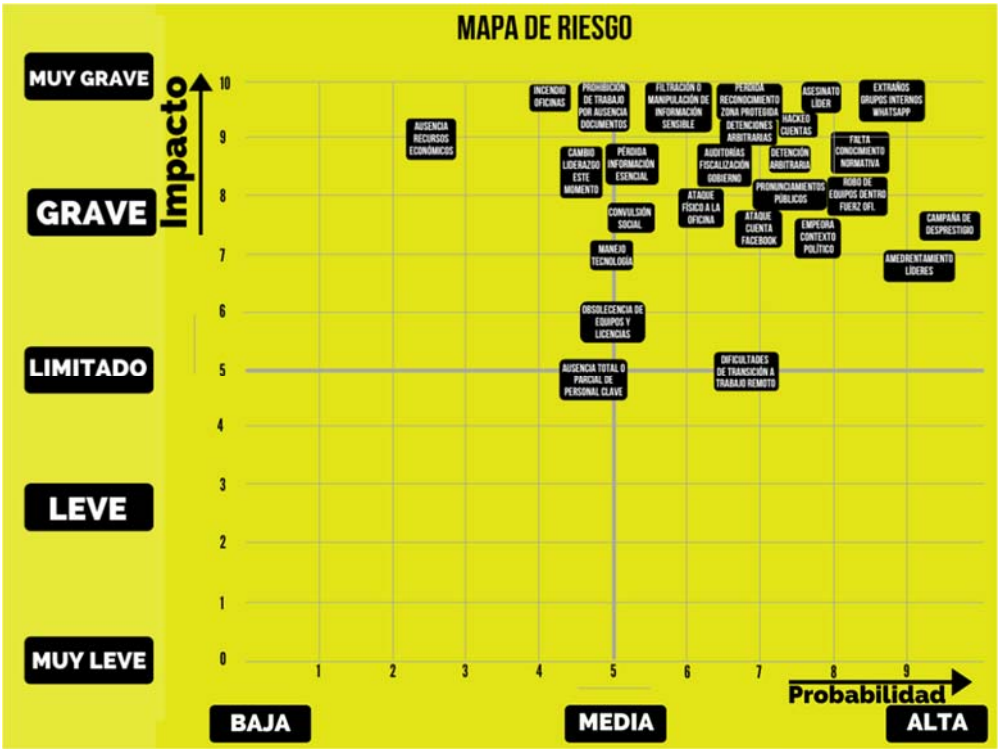


- **Área roja.** Son los riesgos probables y de mayor impacto.
- **Área tomate.** Son riesgos de menor probabilidad, pero un impacto importante.
- **Área amarilla.** Existen menos probabilidad que ocurran y su impacto no es destacado.

La construcción de la matriz debiera ser un proceso pensado, reflexivo, pausado. Se intuyen, analicen en conjunto todos los factores de riesgo; además, escoger el lugar en el que ocupa cada criterio dentro de la matriz. Las decisiones de dónde colocar los riesgos debiera ser consensuado por los participantes y personas destacadas de la organización.

Una vez llenado el mapa no será igual a la de otra organización. Un riesgo de probabilidad alta puede ser bajo para otra. Además, el análisis de contexto determinará también el nivel de impacto. Esta matriz irá variando con el tiempo. Este ejercicio debe realizarse una vez al mes por lo menos. También lo pueden hacer a nivel individual.

Tipos de mapas de riesgos



Algunas metodologías de elaboración de mapa de riesgos colocan impacto en la línea horizontal y probabilidad en la vertical. Otros colocan rangos como: bajo, medio y alto; muy leve, leve, limitado; medio, grave o muy grave. Esto no afecta el criterio de la elaboración de la matriz.

Cualquier tipo de matriz que se elija debe estar claro el código de color rojo, tomate y verde. Los riesgos de color rojo son aquellos que necesitan una acción, un plan de seguridad.

Plan, hábitos, protocolos y uso de herramientas de seguridad

Una vez que identificamos los riesgos se debe pensar en el desarrollo de un plan de seguridad o mitigación de riesgo, la generación de hábitos, protocolos y uso de herramientas de seguridad que atiendan a los riesgos identificados.

Plan de seguridad

Un plan es un conjunto de medidas o lista de pasos para llevar a cabo esa acción de mitigación del riesgo. Estas acciones que llevan a la mitigación de vulnerabilidades. Deben realizarse una vez se conoce los riesgos. No se debe esperar a que un hecho suceda pues el impacto será mayor. Se debe priorizar un plan para aquellas que tienen alta probabilidad de producirse y alto impacto.

Elementos del plan:

- **Riesgos**. Los riesgos catalogados como rojos.
- **Nivel**. Si el riesgo es alto, medio o bajo, de acuerdo con la matriz.
- **Medidas de prevención**. Acciones para implementar para prevenir el riesgo.
- **Plazos**. Corto, mediano y largo plazo con lo que se aplicará la acción.
- **Responsables**. Quién es el responsable de implementarlo.
- **Recursos**. Aquellos recursos que pudieran necesitarse para implementar la acción.

Ejemplo de desarrollo de un plan

Riesgo	Nivel	Medidas de prevención	Plazo	Responsables	Recursos
Infiltrados al grupo de WhatsApp de la organización[1].	Alto	• Indagación y revisión del perfil de las personas que ingresan al grupo. • Revisión de sus perfiles en línea, grupos de contactos, tiempo que se conocen a las personas, etc. Debiera ser un análisis reservado para no levantar sospechas. • La información sensible o altamente sensible no compartirla en grupos de WhatsApp con desconocidos ajenos a la organización. Se puede compartir en persona, sin respaldos, o en canales de comunicación como Signal, con la opción de auto eliminar el mensaje tras un tiempo. • Conocer qué debe hacerse ante pérdida o sustracción de celulares, sobre todo para dispositivos con información sensible. • Implementar procesos de capacitación para la organización donde aprendan protocolos de seguridad digital. • Identificar aliados que puedan capacitar a la organización en seguridad digital.	Corto plazo Corto plazo Corto plazo Corto plazo Mediano y largo plazo Mediano plazo	Persona 1 Persona 2 Persona 1 Persona 3 Persona 3 Persona 1	Número de WhatsApp. Redes sociales. Signal. Manual de pérdida de dispositivos elaborado por la organización. Entrenadores de seguridad digital, presupuesto. Contactos con organizaciones que trabajen seguridad digital.
Falta de conocimiento de la normativa[2]	Alto	• Capacitación en normativa. • Análisis de contexto. • Contactos con abogados y organizaciones aliadas.	Corto plazo	Persona 1	Entrenadores, logística de talleres. Persona a cargo del tema. Contactos.

[1] Muchos defensores de derechos humanos están teniendo comunicaciones sensibles a través de los grupos de WhatsApp. En estos grupos podría infiltrarse personas para recabar información. La misma puede ser utilizada en contra de la organización para afectar la integridad física, digital y emocional de la organización.

[2] La falta de conocimiento de normativa para muchas organizaciones puede constituirse en un riesgo pues a través de ello a veces sus decisiones son manipuladas, no pueden defender de manera efectiva sus derechos, el desconocimiento los coloca en determinadas circunstancias de mayor riesgo de un momento a otro, etc.

La matriz puede incorporar otros criterios tras el análisis de la matriz. Puede reordenarse por grupos de vulnerabilidad; por ejemplo, en lugar de hacerlo de arriba hacia abajo por nivel de riesgo alto a bajo podría reordenarse bajo criterio de seguridad física, digital, emocional, etc. Lo importante del plan es que sea funcional para la organización.

El mapa de riesgos refleja información altamente sensible no es información que pueda compartirse con cualquiera se debe mantener reservada.

Protocolos de seguridad

Una vez identificados los riesgos altos, lo ideal es que no ocurran. Pero sí se debería tener un documento en el que se responda las siguientes preguntas:

- ¿Qué información perdemos, si ocurre un riesgo de color rojo?
- ¿A quién ponemos en riesgo, si ocurre un riesgo de color rojo?
- ¿Qué acciones toma la organización, si ocurre un riesgo de color rojo?
- ¿Qué acciones NO toma la organización, si ocurre un riesgo de color rojo?
- ¿Los dispositivos robados o extraviados, se los formatea a la distancia?
- Cuándo un dispositivo es robados o extraviado, ¿qué contraseñas se cambia?
- Si una persona pierde el acceso a sus cuentas ¿a quién recurre?
- Si una cuenta de la organización es vulnerada o no se puede ingresar, ¿a quién se contacta?
- Si la organización sufre de amenazas físicas o virtuales, ¿qué pasos se sigue?

Política de seguridad

Cada organización debe crear sus reglas o política de seguridad. Respondiendo a preguntas como:

- ¿Cómo manejar información sensible?
- ¿Cómo se clasifica la información de la organización?
- ¿Dónde se almacena la información de la organización?
- ¿Cómo se comparte la información?
- ¿Cuáles son los canales de comunicación de la organización?
- ¿Qué tipo de sistema operativo tiene la organización?
- ¿Cómo se usa los dispositivos de memorias USB de la organización?
- ¿Quién tiene acceso a la clave de Internet de la organización? ¿Se comparte la clave?
- ¿Quién tiene acceso a las redes sociales, correos y sitio Web de la organización?
- ¿Cómo se manejan las redes sociales, correos y sitio Web de la organización?
- Cuando una persona viaja, ¿qué tipo de protocolo de seguridad sigue?
- Cuando una persona viaja, ¿se lleva dispositivos de la organización en el viaje?
- Cuando una persona viaja, ¿se compra un VPN para el viaje?

Hábitos de seguridad

Tras el curso de seguridad. Te recomendamos crear una serie de hábitos de seguridad para tu organización. Acá te compartimos algunos:

- Al salir de la oficina verificar que estén cerradas todas las ventanas de la oficina de manera correcta. Al levantarse de su equipo de computadora verificar que se bloquea la pantalla.
- Verificar regularmente que las actualizaciones están instaladas.
- Prever copias de seguridad al finalizar el mes.

- No permitir insertar dispositivos USB en las computadoras.
- Recomendar no hacer clic en enlaces desconocidos.

Herramientas de seguridad

Se refiere a la previsión de comenzar a usar herramientas con enfoque de seguridad digital, por ejemplo, entre algunas de ellas: gestores de contraseñas; uso de Signal en lugar de WhatsApp para comunicaciones sensibles; conexión con VPN en redes de WiFi público, etc. Esto se lo puede revisar en el curso de seguridad digital.